Constellation Ground Systems Launch Availability Analysis: Enhancing Highly Reliable Launch Systems Design

Jeffrey L. Gernand*, Amanda M. Gillespie†, and Mark W Monaghan‡

Science Applications International Corporation
1710 International Drive
Mclean, Virginia, 22102, USA

and

Nicholas H. Cummings§

Ground Operations Project
National Aeronautics and Space Administration
Kennedy Space Center, Florida, 32899, USA

Success of the Constellation Program's lunar architecture requires successfully launching two vehicles, Ares I/Orion and Ares V/Altair, within a very limited time period. The reliability and maintainability of flight vehicles and ground systems must deliver a high probability of successfully launching the second vehicle in order to avoid wasting the on-orbit asset launched by the first vehicle. The Ground Operations Project determined which ground subsystems had the potential to affect the probability of the second launch and allocated quantitative availability requirements to these subsystems. The Ground Operations Project also developed a methodology to estimate subsystem reliability, availability, and maintainability to ensure that ground subsystems complied with allocated launch availability and maintainability requirements. The verification analysis developed quantitative estimates of subsystem availability based on design documentation, testing results, and other information. Where appropriate, actual performance history was used to calculate failure rates for legacy subsystems or comparative components that will support Constellation. The results of the verification analysis will be used to assess compliance with requirements and to highlight design or performance shortcomings for further decision-making. This case study will discuss the subsystem requirements allocation process, describe the ground systems methodology for completing quantitative reliability, availability, and maintainability analysis, and present findings and observation based on analysis leading to the Ground Operations Project Preliminary Design Review milestone.

Nomenclature

R	=	Reliability
t	=	Time
$R(t)$	=	Reliability at time (hours)
R_S	=	System reliability

* KLXS Operations Lead, Mail Stop: SAIC-LX-4, jeffrey.l.gernand@nasa.gov.
† KLXS RMA Analyst, Mail Stop: SAIC-LX-4, amanda.m.gillespie@nasa.gov.
‡ PhD, KLXS Senior RMA Analyst, Mail Stop: SAIC-LX-4, mark.w.monaghan@nasa.gov, AIAA Member.
§ Technical Manager for Operations Integration, Mail Stop: LX-I, nicholas.h.cummings@nasa.gov.

I. Introduction

THE Constellation Architecture for human lunar exploration missions requires two launches: the Ares V carrying the Earth Departure Stage (EDS) and Lunar Lander and the Ares I lofting the Orion Crew Capsule. The two vehicles are nominally launched 90 minutes apart from Launch Complex-39 pads A and B at Kennedy Space Center (KSC). The architecture permits launching the vehicles in either order, and both the EDS/Lunar Lander payload compliment and Orion have the capability to loiter for a few days in Low Earth Orbit prior to rendezvous and Trans-Lunar Injection. Viability of the two-launch architecture is highly dependent on the reliability and maintainability of ground systems and the flight vehicles, particularly after the first vehicle has launched. Due to limitations in how long the first vehicle can loiter in orbit and successfully achieve the mission, the second vehicle must deliver a very high probability of successfully launching in sufficient time to avoid wasting the first-launched on-orbit spacecraft. Accordingly, the Constellation Program developed a probability of launch requirement that bounded the acceptable risk of mission failure due to a second vehicle launch failure at less than one percent. This requirement stated, "The Constellation Architecture shall have a probability of crewed lunar mission launch of not less than 99 percent during the period beginning with the launch of the first vehicle and ending at the expiration of the last launch opportunity to achieve the targeted Trans-Lunar Injection window."[1] This overarching requirement was decomposed into two child requirements that flowed to each of the Constellation Projects, including the launch vehicle, the spacecraft, and ground systems.

1) The first child requirement stated that the launch vehicle, spacecraft, or ground systems shall have a probability of launch of not less than (a value for ranging between 99 percent and 94 percent, depending on the project) beginning with the decision to load cryogenic propellants and ending with the close of the day-of-launch window for the initial planned attempt. This critical time period was originally estimated at about fourteen hours, and then later revised to ten hours.**
2) The second child requirement stated that in the event of a failure, the launch vehicle, spacecraft, or ground systems must deliver a probability of repair of some percentage of not less than (a value for ranging between 30 and 45 percent, depending on the project) in order to be prepared to support at least one additional launch attempt within an acceptable time period (approximately three days).

At first consideration, the child requirements would seem inconsistent with the parent requirement for the architecture to deliver not less than a 99 percent chance of success. For example, if the launch vehicle and the spacecraft each delivered a 98 percent probability of success and ground systems delivered a 99 percent probability of success, the architecture would deliver only a 95 percent probability of success. This is true only for the first launch attempt. The second child requirement, which defines the maintainability standards, enables a likelihood of a second launch attempt in the event of a launch failure. The combined likelihood of a successful repair and at least one additional launch attempt enables the architecture to satisfy the overarching requirement to deliver a probability of successful launch within the acceptable time period of not less than 99 percent. The Constellation architecture and the launch probability requirements flow is illustrated in Figure 1.

This paper describes how the Constellation Ground Operations Project (GOP) applied quantitative Reliability, Maintainability, and Availability (RMA) theory, tools, and techniques to allocate launch probability requirements and to assess compliance with those launch probability requirements for the Constellation Ground System. Additionally, the paper describes how the launch probability assessment was leveraged and translated into assessing maintainability of the Ground System, evaluating compliance with the second child (maintainability) requirement, and focusing efforts on logistics support and operations planning.

It should be noted that, due to the sensitivity of the detailed analysis products, specific subsystem analysis results, subsystem names, and specific descriptive information have been generalized. However, specific analysis results are provided to demonstrate the analysis process and the benefits of the effort. Information contained within this report was developed prior to the GOP Preliminary Design Review (PDR) milestone.

** Although there were two iterations of critical time period duration and changes to subsystems included in the analysis, for consistency, the final critical time period value of 10 hours and the final configuration of ground subsystems are used throughout this paper.

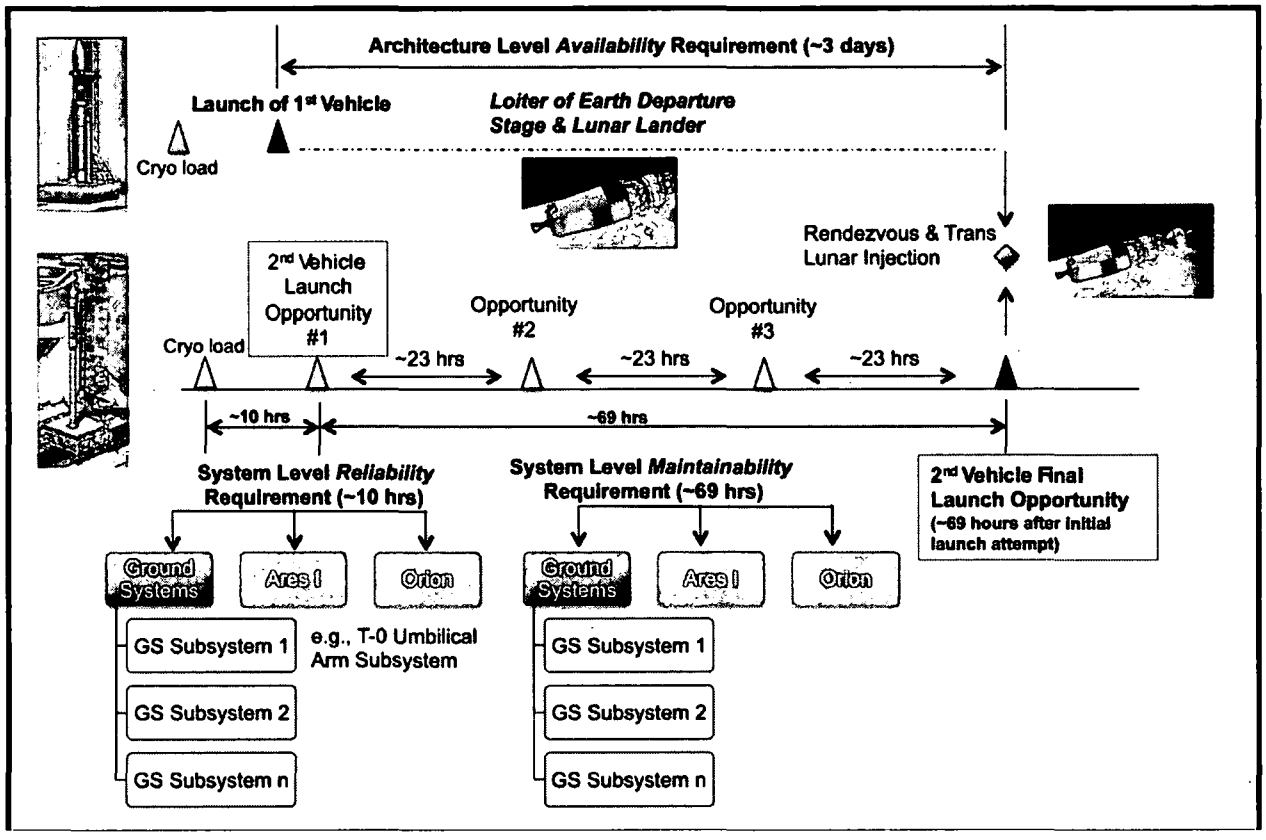


Figure 1. Constellation 2-Launch Lunar Architecture and the Associated Launch Probability Requirements Flow to Ground Subsystems

II. Phase I - Ground Systems Requirements and the Initial Allocation Process

Constellation GOP was allocated a requirement to deliver not less than a 99 percent probability of launch. In other words, Constellation requirements dictated that no more than one in 100 launch attempts could be scrubbed due to a failure of the Ground Systems after the point loading of cryogenic propellants is initiated. Historically, throughout the Space Shuttle Program, tanking for launch was initiated approximately 205 times and there have been approximately 24 instances where the planned launch time was delayed due to ground systems faults.[2] Accordingly, Ground Systems delivered an approximately 88 percent probability of successful launch support throughout the Space Shuttle Program. The Constellation architecture requires significant improvements in the reliability of its ground systems versus the Space Shuttle ground systems.

In response to the requirement to deliver not less than a 99 percent probability of launch, the Constellation GOP developed an approach to decompose and allocate launch availability requirements to the subsystem level of the Ground System. This method was not standard requirements flow practice since it bypassed the intermediate "Element" level in the requirement flow down. The benefit of this direct approach was in aligning the launch availability analysis with the subsystem design review process and the subsystem design team structure.

The initial requirements allocation analysis consisted of determining which ground subsystems would be included in the analysis. The determination was based on the sole criteria that a failure in the subsystem could result in a launch hold or scrub during the critical time period between cryogenic propellant loading and launch. Since a failure within each selected subsystem could cause a launch hold or scrub, all subsystems within the probability of launch analysis were considered in series. The reliability of a number (n) of components in series at a given time is the product of the reliability of those components, as shown in Eq. (1).

$$R_S = R_1 * R_2 ... * R_n \quad (1)$$

In order to assess where the general quantitative requirement values should be, the RMA team applied Eq. (1) to determine the required reliability for n=55 identical subsystems in series to deliver a 99 percent probability of launch. Equation (2) shows the calculation and the results.

$$R_{1\to n} = \sqrt[n]{R_s} = \sqrt[55]{0.99} = .999817 \quad (2)$$

As a result of this simple analysis, several factors became apparent, including the following:

1) Given the limited knowledge of actual subsystem performance or design at the time, launch availability requirements were allocated as "order of magnitude" requirements (such as 0.999, 0.9999, 0.99999, etc), at least initially.
2) If approximately 55 ground subsystems were all required to operate successfully through the critical time period, the vast majority of these subsystems would need to deliver at least 0.9999 availability through the critical time period.
3) Since the overall result was multiplicative, no subsystem could deliver less than 0.99 availability and successfully meet the overall ground systems 99 percent probability of launch requirement. Only a very small number of systems delivering 0.999 availability could be tolerated.

Based on the observations above, subsystems that met the launch hold or scrub criteria were subjected to further analysis to determine the following:

1) If the subsystem was repairable within the operational constraints of the launch time frame. For example, once propellant loading begins, access to the launch pad area becomes extremely limited. If a repair is required within the clear area, the launch is generally scrubbed, propellants are drained from the vehicle, and access is restored after confirming a safe work environment. Subsystems within this launch clear area would be analyzed for subsystem *reliability* during the critical period since repairs could not contribute to subsystem *availability*. Subsystems with components located outside the launch clear area received credit for repair capabilities during the countdown in the event of a failure, if the repair could reasonably support the countdown time limitations.
2) If the subsystem was inherently high or low availability. High availability subsystems would be required to deliver not less than a 99.99 percent probability of successful operation through the critical time period. Low availability subsystems would be required to deliver not less than a 99.90 percent probability of successful operation through the critical time period. Factors indicating that a subsystem should be designated as high availability included subsystem criticality, redundancy, reparability, and/or demonstrated highly reliability performance. Factors indicating a low availability designation included non-reparability, low historical performance, low redundancy, and/or design risk. Subsequently, a third category (very high) was added for subsystems that, due to their construction, were so monumental that a failure was extremely unlikely. Facility structures such as flame chutes, launch mounts, and lightning towers typically populated this new category. These subsystems were assigned a requirement of 99.999 percent probability of successful operation through the critical time period.[3]

The RMA team developed an initial matrix that summarized all of the ground subsystems, the KSC organization responsible for the design, whether the system was included in or excluded from the analysis and why, whether or not the system was repairable, and an initial high, low, or very high availability allocation for "included" subsystems. This matrix was continuously refined with input and support from various subject matter experts from the Space Shuttle Launch Operations Team, Ground Systems design teams, and Safety and Mission Assurance staffs. Support from each of these organizations was superb with each stakeholder organization contributing significantly to the quality and clarity of the final allocation. In this process, adjustments were made, assumptions were challenged, and the refined requirements were formally allocated into subsystem design requirements.

Of the 80 subsystems that made up Constellation Ground Systems[4]:

- 25 subsystems were excluded as they were evaluated as having no impact on launch availability within the critical time period
- 2 subsystems were evaluated as low availability
- 48 subsystems were evaluated as high availability
- 5 subsystems were evaluated as very high availability due to the extremely low probability of structural failure within the critical time frame

Overall, 55 subsystems were identified for subsequent launch availability analysis. A simple reliability calculation was used to assess Ground Systems' overall launch availability if each of the 55 subsystems met their allocated launch availability requirement through the 10 hour critical time period. It is important to restate that the sole criterion for selecting a subsystem for inclusion in the launch availability requirement and analysis process was that a failure in the subsystem could result in a launch hold or scrub. This would indicate consistency with independent failure theory and calculation techniques, since a single subsystem failure would cause a complete ground systems failure. The calculation and the results shown in Eq. (3) provided an initial assessment that the allocated subsystem requirements exceeded the overarching Ground Systems requirement of 99 percent. Therefore,

if each subsystem meets or exceeds its allocated availability requirement, overall Ground Systems will meet or exceed the second launch availability requirement.

$$R(10hrs) = (0.999)^2 * (0.9999)^{48} * (0.99999)^5$$
$$R(10hrs) = .993172 \quad (3)$$

The allocation method and results described above were highly favorable for the following reasons:

1) The order of magnitude differences between the low, high, and very high allocations were appropriate, since predicting the availability of complex subsystems is not a precise process.
2) Refining the allocations beyond the order of magnitude measures added little value for the design engineer, at least initially.
3) The excess 0.003172 provided management reserve or growth margin to address unexpected developments that may occur during the ground system development process. Within the management reserve an additional three "low availability" subsystems and one "high availability" subsystems could be added (or two "low availability" and 11 "high availability" subsystems could be added, etc.) and still meet the overall Ground Systems 99 percent launch availability requirements. This also provided the ability to accommodate some limited cases where subsystems failed to meet the allocated launch probability requirements.

Phase-I was completed when allocated launch availability requirements were approved by GOP decision makers. The initial requirements were revised over time to add and remove subsystems, as required, as the Project and the associated designs matured.

III. Phase II – Subsystem Analysis

When approved probability of launch requirements were formally allocated to the subsystem level, the analysis effort began to assess each of the subsystems' compliance with the requirements. Requirements verification language specified the use of quantitative analysis techniques to assess and validate compliance with the overarching probability of launch requirements. In constructing the analysis methodology, the GOP RMA team envisioned the following key outputs of the analysis and the associated products:

1) A quantitative estimate of subsystem reliability (or availability for systems that could be repaired within the critical time period) for the critical time period using a 95 percent confidence interval.
2) Clear documentation of the analysis assumptions. For example, if the subsystem analysis assumed that a launch countdown would continue if one of two redundant paths failed, the assumption would need further validation within the Launch Commit Criteria process.
3) Recommendations for potential improvements in subsystem predicted performance early in the design in the process, when adjustments are easier to make and are less costly.
4) An initial look into potential logistics support priorities, understanding that a more detailed maintainability analysis would follow in the Phase III analysis.

These key outputs were envisioned to support informed decision making as new design subsystems were developed. Additionally, several legacy subsystems were allocated launch probability requirements, as they would also be required to support Constellation launch operations. Therefore, Phase II launch probability analysis would inform decisions regarding design alterations to both new and legacy subsystems. In addition to design changes, other methods to improve launch probability would be considered, such as adjustments to operational limits, procedural concepts, or adjustments to the launch availability requirement for the subsystem within the available trade space.

The GOP RMA team evaluated a number of tools and techniques to meet the analysis requirements. Discrete Event Simulation (DES), Probabilistic Risk Assessment (PRA), and classic reliability and maintainability techniques were among the techniques considered. In order to produce quantitative outputs described above based on subsystems design, component failure data, and the subsystem configuration, the clear choice in developing the RMA team's approach was to apply classic reliability and maintainability techniques.

Recognizing that KSC's ground systems were highly complex and many had built in redundancy or stand-by features, the more simplistic classical RMA parts counts methodologies would not produce accurate reliability estimates. Parts count methodologies essentially assume that all parts exist in series and that any failure will cause system failure. Therefore, the Reliability Block Diagram (RBD) analysis method was selected since it appropriately addressed subsystem functionality, operability, maintainability, and redundancy.

A. Analysis Tool Background

KSC's Integrated Design and Assurance System (IDAS) project provided an excellent source of information, support, and tool suites to address a wide variety of reliability and assurance activities. The IDAS web site explains that, "IDAS shares and supports tools that perform technical analysis for the design, system, safety, mission assurance and sustaining engineering functions over the life cycle of a system. In addition, IDAS collects and shares information that helps the engineer or analyst to learn and apply the tools and techniques."[5] IDAS also provided access to a variety of reliability software suites. One of those suites, an RMA-focused software package, delivered a broad spectrum of design, development, and life-cycle RMA analysis tools. This software was readily available to KSC users through the Center network, along with user support, training, and technical resources through the Center's support contract with the vendor.

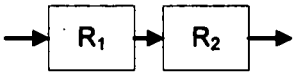
The Constellation GOP RMA team primarily uses this software suite in support of the probability of launch availability and maintainability analyses. In this effort, the most commonly used reliability software modules are the Reliability Prediction and RBD modules. The GOP RMA team also uses the Weibull capabilities to develop failure rates using historical data from various failure reporting and corrective action systems. In order to understand the analysis process and the underlying methodology, a brief primer will be useful to set the stage for the subsequent discussion.

RBD techniques form the foundation of the GOP launch availability and maintainability analysis. An RBD is a symbolic logic model that depicts system functionality and operates in the success domain. Each RBD has a specific start and a specific end. Each block within the RBD may represent an individual component, such as a resistor or screw, or blocks may represent components and/or assemblies at a higher level, such as an entire automobile engine or a complete pump, if sufficient reliability (and repair) data are available. Each RBD block captures the failure and repair parameters of each element within the system.

RBD blocks are connected functionally to replicate the system's operational characteristics. Blocks are connected in series if each element is required for the system to operate. Parallel branches are used when only a subset of the depicted branches is required. This would be used when only one of two (or two of three, etc.) parallel branches are required to operate the system successfully.

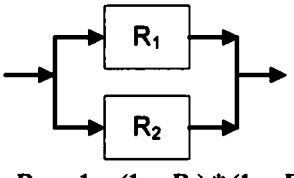
The examples below depict several representations of simple RBD configurations and their associated reliability calculation formulae are provided in Eqs. (4) and (5).

Series



$$R_S = R_1 * R_2 \tag{4}$$

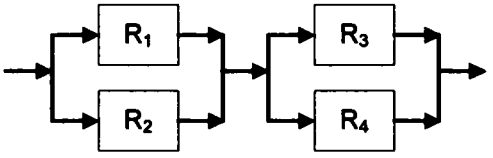
Parallel



$$R_S = 1-(1-R_1)*(1-R_2) \tag{5}$$

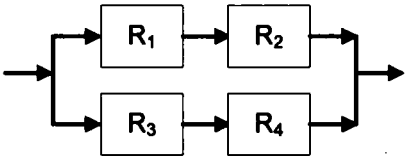
The concepts and mathematical relationships from the basic building blocks above are applied to calculating the reliability of more complex systems. In application, variations and combinations of these of these basic patterns are used to depict the components of a system, the interconnections, and how they interact as the system operates as shown in Eqs. (6) and (7) below.

Series-Parallel



$$R_S = (1-(1-R_1)*(1-R_2))*(1-(1-R_3)*(1-R_4)) \quad (6)$$

Parallel-Series



$$R_S = 1-(1-R_1*R_2)*(1-R_3*R_4) \quad (7)$$

The second key reliability software module used in the GOP launch availability effort is the Reliability Prediction module. This portion of the software shares data with many other packaged modules, including the RBD module. The Reliability Prediction module was used to capture and store failure and repair data for parts, components, and assemblies used in an associated RBD.

The software tool Reliability Prediction module can be used to develop parts listings from user input data or from parts libraries such as MIL-HDBK-217 for electronic parts, Reliability Analysis Center's handbook NPRD-95 for non-electronic parts, and NSWC-98 "Handbook of Reliability Prediction Procedures for Mechanical Equipment." These capabilities allow the user to develop a complete parts library for the specific system based on a variety of different sources and techniques. The Reliability Prediction module also supports multiple failure and repair distributions.

Since the Reliability Prediction module shares data with the RBD module (and others), components in the parts library can be pulled into the RBD as it is developed. This feature improves the ease of RBD construction and the accuracy of the RBD data. A single part in the library may be used multiple times in the system being modeled, but if the failure rate needs to be updated based on new data, this only needs to be done in the Reliability Prediction module, with the RBD being updated automatically upon calculation of the reliability of the system.

B. Analysis Methodology

The GOP RMA team initially encountered a significant amount of skepticism early in the project. Throughout the initial allocation process, a number of concerns were voiced by the various stakeholders. The most frequent concerns were:

1) "Meeting these requirements will drive cost through the roof."
2) "The design teams are already overtaxed. This RMA work will create huge burdens on the design teams and detract from the real work within the design effort."
3) "There's no way we will ever meet this requirement for 99.99 percent reliability at the subsystem level."
4) "We think you did the math wrong on the allocation process."

Through several weeks of discussion, stakeholders developed a better understanding of the analysis objectives and the RMA team developed a better appreciation for their concerns. Accordingly, a methodology was developed that was focused on achieving the following objectives:

1) Introduce the RMA team as an embedded member of each design team and as a resource to the design team.
2) Minimize the time impact on the design team by developing an independent understanding of the design package within the RMA team and using the design team only for clarification or confirmation that the model and underlying assumptions were correct.
3) Link the RMA analysis to the design review milestones, wherever possible, and include the Launch Availability Analysis report as a reviewable document within the design package.

4) Provide feedback to the design team, such as reliability improvement recommendations, throughout the design process and deliver no surprises to the design team in the final analysis. This includes supporting the design effort by evaluating alternative solutions from a system reliability perspective.

In execution, these objectives were largely achieved by following a similar process through each subsystem analysis. First, an analysis schedule was developed based on the subsystem design review schedule. Launch availability analyses supported the 60 percent, 90 percent, and 100 percent design reviews for each subsystem with an allocated probability of launch requirement.[††] Each analysis was documented in a peer-reviewed report. The analysis followed the following general process:

1) The design package was made available to the RMA team electronically.
2) The RMA team reviewed the design package to become oriented with the subsystem functionality, operations concepts, and specific design. The following documents and data sources within the design review package were assessed within the launch availability analysis:
    a. Operational Concept Documents
    b. System Assurance Analysis (SAA) – which included fault tree and hazard analyses
    c. Drawings and Schematics
    d. Parts information and listings
    e. Logistics Support Analysis (LSA)
    f. Interface diagrams and tables
    g. Launch Commit Criteria documentation
    h. Subsystem training plans
    i. Lessons learned reports
    j. Procurement specifications
    k. Subsystem Requirements Documents
3) Based on the integrated understanding of subsystem functionality, operating profile, and risks developed during the design package review, the RMA team decomposed the subsystem to an appropriate level, developed functional flow diagrams, and produced initial parts listings specific to the design. The flow diagrams reflected the operational usage, system layout, connectivity, and redundancy schemes, and formed the basis for subsequent RBD development. Frequently, several functional flow diagrams would be required to capture the necessary scope of the subsystem.
4) Having developed an initial understanding of the subsystem operation and functionality, the RMA team conducted an initial meeting with the design team to confirm that there was a correct understanding of subsystem operations, confirm or revise functional flow diagrams, resolve questions, review the parts listing, if required, and to determine if any subsequent design changes were in work for the design release. These initial meetings normally lasted one to two hours. The knowledge of the design team was instrumental in accurately capturing how the subsystem operates, which components need to be included in the reliability analysis, the associated failure data, and how to best map the subsystem configuration in the RBD.
5) Building on the knowledge developed and a common understanding (with the design team) of the subsystem operation, layout, components and assumptions, the RMA team refined the parts list and the associated failure and repair data for each modeled component or assembly. This information was catalogued in the associated software Reliability Prediction module for the subsystem. Failure and repair data was compiled using the following information sources to determine the most accurate and most applicable data:
    a. Manufacturer's data for the specific part
    b. Failure data develop from like-comparison failure histories
    c. Parts libraries
    d. Other reference materials such as IEEE Std 493-2007, IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems
    e. Test data
    f. Reliability prediction techniques
6) RBDs modeling the subsystem were then developed using the information from the functional flow block diagrams and the reliability and repair data contained for each component or assembly in the

[††] Not all subsystems followed the 30, 60, 90, and 100 percent design review process. A few subsystems deviated with other design review milestones such as 45 and 90 percent. The Legacy subsystems usually did not have any associated design review milestones.

associated parts library in the Prediction module. All components analyzed within the RBD were considered to be operating at optimum level and conditions until a failure occurred. The configuration of all components within the RBD determined if the system's success was dependent on one or more component failures. The blocks of the RBD may represent individual components or component substructures, which in turn may be represented by other RBDs. The complexity of the RBDs is dependent upon various factors such as mission profiles, function criticality, and redundancy characteristics.

7) Initial estimates were developed using the RBD module Monte Carlo simulator for the 10 hour critical time period and a 95 percent confidence interval. Normally, one million Monte Carlo simulations were executed. The results were examined and peer reviewed by the RMA team to verify that all connections were correctly made, the correct parts were in the correct locations, the parts data were correctly entered, and that the RBD functioned as depicted in the functional flow diagram.
8) Initial observations were developed and shared with the design team during a second feedback session. RMA team observations shared with the design team frequently included:
    a. Reliability improvement recommendations
    b. Drawing corrections
    c. High failure rate nodes within the design
    d. Design inconsistencies
    e. GIDEP alerts on parts specified for use
    f. Obsolete parts specified for use
9) The analysis report was then developed in support of the design review schedule. A documentation scheme was developed that captured the RMA requirements compliance verification process[6] and verification of probabilistic requirements using a six step process.[7]
10) After peer review and further coordination with the design team, the report was loaded into the design review package as a reviewable and commentable document.

C. Launch Availability Analysis Observations

At the GOP PDR milestone, 29 of the 55 subsystems with allocated probability of launch requirements had been analyzed at least once. Most of the analyzed subsystems were new design subsystems and a few were legacy subsystems. Analysis priority was given to the new design subsystems and supporting their multiple design reviews over the legacy subsystems.

Across the 29 analyzed systems, the following facts emerged leading into the PDR:

1) 22 of the 29 subsystems met or exceeded their allocated launch availability requirements
2) 7 of the 29 subsystems fell slightly short of meeting their launch availability requirements
3) Overall, the 29 evaluated subsystems delivered a 0.9966 probability of launch. The net requirement for these 29 subsystems was to deliver not less than 0.9953 launch availability.
4) If the remaining 26 subsystems met or exceeded their allocated requirements, the GOP would deliver an overall launch availability of 99.44 percent, exceeding the overarching requirement.

Although the launch availability assessment as of PDR indicated that Constellation Ground Systems was on track to meet or exceed the 99 percent probability of launch requirement (with 95 percent confidence), additional analysis of the reliability growth through the process provided more insight into the impact of the RMA process on the subsystem designs. Of the 29 analyzed subsystems, nine were reviewed more than once. The reliability growth calculated for each of these nine subsystems as they progressed through multiple reviews is summarized in Table 1. The results indicate the following about subsystem reliability improvement using the methodology stated in this paper:

1) On average, the RMA and design teams improved the reliability of subsystems by a factor of 9.3. This result is the ratio of the average improved design MTTF over the average original design MTTF.
2) The reliability improvement results in Table 1 are understated for two reasons:
    a. Many design improvements were often incorporated into the initial design packages as a result of the initial launch availability analysis.
    b. The 10 hour subsystem availability value was "capped" at no better than 0.999999. Several subsystems had better estimated performance.
3) The first subsystem in Table 1 is indicative of improvements achieved in a subsystem without reliability improvement included into the initial design package. Due to the timing of this design package, little or

no RMA team input to design reliability was incorporated into the initial design package. In this case, the reliability improvement factor was estimated at about 250.

Subsystem	Initial Reliability	Reliability Improvements Implemented	Initial MTTF (hrs)	MTTF (hrs) Improvements Implemented	Reliabilty Improvement Factor
1	0.999750	0.999999	39,995	9,999,995	250.0
2	0.999930	0.999999	142,852	9,999,995	70.0
4	0.999940	0.999999	166,662	9,999,995	60.0
5	0.999885	0.999970	86,952	333,328	3.8
6	0.999997	0.999999	3,333,328	9,999,995	3.0
7	0.999915	0.999965	117,642	285,709	2.4
8	0.998363	0.999207	6,104	12,605	2.1
9	0.999981	0.999983	526,311	588,230	1.1
	0.997762	0.999121	552,481	5,152,482	49.1
	Composite Reliability (R1*R2*R3...*R9)		Average MTTF		Average Improvement Factor

Table 1. Reliability Improvement of Subsystems with Multiple Reviews

4) The average of the nine reliability improvement factors indicates an average improvement factor of 49 across the nine subsystems with multiple reviews.

In each of the nine cases, subsystem availability improved as a direct result of the implemented approach and methodology. In the analysis of each of the first 29 Ground Operations subsystems, performance improvements were made by identifying the follow types of problems:

1) Adding redundancy to key failure nodes
2) Clearly identifying and challenging which functional elements of the subsystem were actually required to support launch countdown
3) Clarifying or establishing operational criteria, such as, two of three "strings" within the subsystem must be operable to continue the countdown
4) Replacing obsolete parts or components within the design with current or improved parts
5) Identifying manufacturer parts with better performance for key failure nodes
6) Identifying linked nodes of failure that will reduce the effectiveness of existing subsystem redundancy
7) Identifying inconsistencies across multiple subsystems.

Additionally, reliability improvements that were identified within one subsystem were sometimes carried across multiple subsystems designs. For example, the RMA team discovered that the greatest contribution to the unreliability of one subsystem was from the power scheme. This power scheme was used within many other subsystems designs. Working with the subsystem designers, the RMA team evaluated and recommended potential power scheme improvements based on quantitative reliability results. The most suitable power scheme configuration was then propagated through other subsystem designs, improving their performance and overall GOP launch availability.

IV. The Maintainability Requirement

As the launch availability methodology was refined, the GOP RMA team developed a second methodology to assess subsystem maintainability and compliance with the requirement that in the event of a failure, ground systems must be able to repair at least 30 percent of the failures and support readiness for launch within a limited time period (69 hours). This requirement was flowed directly to each ground subsystem with an allocated launch availability requirement less stringent than 0.99999.

The methodology to assess subsystem maintainability leveraged the subsystem RBD already developed under the launch availability analysis. If the RBD could be used to show the relative likelihood of the various failure paths, then repair scenarios could be evaluated for the most likely failures. Fault Tree Analysis uses a similar technique

called cut set analysis. The RMA team found the best explanation of cut sets to be "unique combinations of component failures that can cause system failure."[8] The article further defined a *minimal cut set* as "when any basic event (failure of a component) is removed from the set, the remaining events collectively are no longer a cut set."[9] Minimal cut sets can be used to understand the likelihood of a subsystem failure. Essentially, minimal cut sets define all of the combinations of component failures that result in system failure. Minimal cut sets may consist of one of more components. For complex or redundant systems, minimal cut sets can (and do) number in the millions. By defining each component within a cut set, the analyst can calculate the likelihood of all events occurring within a stated time period. In this application, cut sets are used to evaluate subsystem *unavailability*.

As an example, consider a system that can fail in 1,000 different ways. Each failure path may contain any number of components, from one to many. Each of those failure paths are defined by the components that contribute to the failure path and by the failure data for each of the contributing components. Unavailability can then be calculated for each failure path within the given time period. The cut set results can be numerically ordered, for example, from the highest unavailability to the least for each of the 1,000 failure paths. This shows the analyst the quantitative estimate for each failure path and the relative likelihood of the failure occurring within the system.

The reliability software package used by the RMA team delivers the ability to produce cut set analysis from within the RBD module. Therefore, cut sets derived from an RBD can be used to determine each failure path that causes the system to fail and the combined unreliability of those components within each cut set. Since this is a calculated value based on the failure data for each component (retained in the RBD and the associated parts library), the unreliability of each failure path can be calculated as a point estimate, and the composite cut set listing can be rank ordered from most likely to least likely to occur. Additionally, since the unavailability associated with each cut set is a calculated value, they can be readily compared within the subsystem, and since each subsystem could individually create a hold or scrub if it failed, cut sets can be compared and ranked across ground subsystems.

A. Cut Sets - Easier Said Than Done

The complexity of KSC's ground systems required developing very sophisticated RBDs. Some complex subsystems were modeled with over 3,000 blocks. In order to organize such systems, the software package RBD module provides the capability to create "linked diagrams" within an RBD. This allows a top level outline level RBD to be decomposed into one or many linked diagrams where lower levels of detail are developed and displayed. This technique does not create problems with the RBD module reliability or availability calculations. It does, however, create problems in developing integrated cut set results within complex systems that use linked diagrams.

The GOP RMA team observed that the software would not calculate cut set results for linked diagrams. However, cut sets could readily be developed for lower level diagrams as long as a linked diagram was not included. The RMA team presented this issue to the vendor to resolve. As of the date of this report, resolution of the cut set compilation problem was ongoing by the vendor. In the meantime, a more labor intensive work-around was successfully developed to gather, compile, and rank cut set output using a spreadsheet in order to complete the maintainability analysis process.

B. Cut Set Analysis Results

Leading up to the PDR milestone, the RMA team had successfully evaluated cut set results for 15 subsystems. Several subsystems produced millions of cut sets. One complex and highly redundant subsystem produced over 2 billion cut sets. Due to the complexity of managing millions of cut sets and the extremely low probability of many of the possible failure paths, cut sets with unavailability less than $1x10^{-16}$ (point estimate) were not included in the analysis. Table 2 shows the cut set results for these 15 subsystems.

The results show that for many of these systems, most of the failures come from a very limited number of failure paths. On average, about one-tenth of one percent of a bounded set of all possible failure paths (only those cut sets with greater than $1x10^{-16}$ unavailability) caused about 30 percent of the subsystem unavailability. Less than one percent of these paths caused about 90 percent of the failures.

Although the RMA team expected that most subsystem failures would come from a limited number of sources, these results were surprising. The implications of this analysis for reliability improvement and validation of the maintainability requirement were also highly significant. When a small number of failure paths make such large contributions to subsystem unavailability, isolating the key failure paths becomes obvious. Even in a complex system with thousands of components, the cut set analysis clearly shows the most likely paths. This enables the design team to focus on either:

1) Improving the design to correct the high failure nodes (improving reliability), or

2) Ensuring that the component is as repairable as possible (improving maintainability) by ensuring that access is to the component(s) is readily available, appropriate spares are established, and repair procedures are developed and tested.

Cut set analysis provides clear indication of where the most likely failure paths would be depending on the accuracy of the RBD that depicts the subsystem arrangement and the accuracy of the failure data contained within the parts library.

Subsystem	Subsystem Reliability	Number of Cut Sets (Unavailability > 1E-16)	Number of Cut Sets (30% of Subsystem Unavailability)	Percentage of Cut Sets (30% of Subsystem Unavailability)	Number of Cut Sets (90% of Subsystem Unavailability)	Percentage of Cut Sets (90% of Subsystem Unavailability)
a	0.999999	1,751	9	0.51%	211	12.05%
b	0.999239	29	1	3.45%	12	41.38%
c	0.999319	32	1	3.13%	13	40.63%
d	0.999671	39	2	5.13%	20	51.28%
e	0.999721	13	1	7.69%	7	53.85%
f	0.999974	692	1	0.14%	3	0.43%
g	0.999983	270	1	0.37%	4	1.48%
h	0.999999	393,480	390	0.10%	1,150	0.29%
i	0.999938	5,729	9	0.16%	36	0.63%
j	0.999997	263	1	0.38%	11	4.18%
k	0.999885	28,653	12	0.04%	121	0.42%
l	0.999825	15	1	6.67%	3	20%
m	0.999488	2,908	1	0.03%	292	10%
n	0.999358	968	30	3.10%	40	4%
o	0.999999	20	1	5.00%	3	15%
		434,862	461	0.11%	1,926	0.44%
		Total		Total Average	Total	Total Average

Table 2. Cut Set Analysis Results for Fifteen Subsystems

V. Conclusion

The work accomplished by the Constellation Ground Operations RMA team in conjunction with the many contributing design teams was instrumental in developing and assessing compliance with quantitative requirements for both probability of launch and subsystem maintainability. The analysis methodology produced results that were highly repeatable and auditable. The process made significant and measurable contributions to ground systems reliability. As of the Constellation Ground Operations Project Preliminary Design Review milestone, the GOP was on track to exceed the requirement for Ground Systems to deliver a 99 percent probability of launch for the second launched vehicle in the Constellation architecture. If the Space Shuttle Program ground systems design effort was able to achieve similar improvements in ground system launch availability as shown in this report, Shuttle ground systems performance could have improved from the historical 88 percent to at least 98.6 percent launch availability. In planning to recover from a launch scrub, the maintainability analysis using cut set techniques clearly identified the most critical failure nodes and where resources could be best applied to evaluate subsystem improvement (to prevent the problem) or to improve the subsystem maintainability (to successfully recover). This analysis is highly adaptable and usable across a wide variety of RMA applications.

Appendix A
Acronym List

DES	Discrete Event Simulation
IDAS	Integrated Design and Assurance System
GIDEP	Government-Industry Data Exchange Program
GOP	Ground Operations Project
GS-SRD	Ground Systems - Systems Requirements Document
MTBF	Mean Time Between Failure
MTTF	Mean Time to Failure
PDR	Preliminary Design Review
PRA	Probabilistic Risk Assessment
RBD	Reliability Block Diagram
RMA	Reliability, Maintainability, and Availability

Appendix B
Glossary

Reliability	The probability that a component or system will perform its intended function with no failures for a given period of time when used under specified operating conditions.
Maintainability	The probability a failed item will be restored or repaired to a specified condition within a given period.
Availability	The probability that a repairable system will perform its intended function at a given point in time or over a specified period of time when operated and maintained in a prescribed manner. Thus, availability is a function of reliability and maintainability.

Acknowledgments

The authors wish to acknowledge Timothy C. Adams, an employee of the Kennedy Space Center and a Certified Reliability Engineer, for his support and mentorship of the RMA team as the methodologies and practices described within this paper were developed and implemented. Tim was, and continues to be, a tremendous asset to the team and a great sounding board for developing new approaches to long standing challenges.

References

[1] NASA, *CxP 72006 Ground Systems System Requirements Document,* Kennedy Space Center, FL, 2007.
[2] Cates, G., *Shuttle Probability of Launch,* Kennedy Space Center, Florida, 2009.
[3] NASA, *GOP-00-1031 Ground Elements Launch Availability Requirements Phase 1-Subsystems Initial Allocations Final Report,* Washington, DC, 2008.
[4] NASA, *GOP 400005 Ground Elements Master Subsystems List,* Baseline Version, Kennedy Space Center, FL, 2008.
[5] Adams, Timothy C., NASA: Kennedy Space Center, *Systems and Reliability Engineering.* URL: http://kscsma.ksc.nasa.gov/Reliability/Default.html [cited February 2, 2010]
[6] NASA, *CxP 70087 Constellation Program Reliability, Availability, and Maintainability Plan,* Washington, DC : NASA, 2007.
[7] Singhal, Surendra N., *Best Practices for Overall Verification of Probabilistic Engineering Requirements,* Washington, DC : 2007.
[8] Hotwire, *Reliability Basics - Minimal Cut Sets Definition,* URL: http://www.weibull.com/hotwire/issue63/relbasics63.htm [cited February 16, 2010]
[9] ibid
[10] Ebeling, Charles E., *An Introduction to Reliability and Maintainability Engineering,* Long Grove, IL, Waveland Press, 2005.

[11] Reliability Analysis Center, *Reliability Toolkit: Commercial Practices Edition*, Rome, NY, Reliability Analysis Center, 1994.
[12] Reliability Information Analysis Center, *Handbook of 217Plus Reliability Prediction Models*, Utica, NY, Air Force Research Laboratory, 2006.
[13] Benbow, Donald W. and Broome, Hugh W., *The Certified Reliability Engineer Handbook*, Milwaukee, WI, ASQ Quality Press, 2008.
[14] Koval, D. O., *IEEE STD 493-2007: IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*, New York, The Institute of Electrical and Electronics Engineers, 2007.